内部情報セキュリティ強化と企業パフォーマンスの向上に関する試論

―― 個人情報保護法と企業に求められる戦略的情報マネジメントとは ――

Essay on Enforcement of Internal Information Security and Improvement of Corporate Performance

―― Act for Protection of Personal Data and Strategic Information Management required to Corporation ――

小笠原　泰☆
Yasushi Ogasawara

【要　旨】

2005年4月から「個人情報保護法」が全面施行されることで，民間企業に対しても同法の適用が開始され，同法に違反した企業には法的罰則が課されることになる。内部情報漏えいは，これまでも企業にとって大きな損失でありリスクマネジメントの対象であったが，今後は，より厳格な内部情報セキュリティ対策を講じる必要が生じてくる。内部情報セキュリティ対策の強化は，一般的に，モチベーションや生産性の低下など，「負」のイメージで捉えられることが多いが，情報マネジメントという観点からの，戦略的な導入によっては，業務刷新，ナレッジマネジメント，組織再設計を通した企業パフォーマンスの向上をもたらす経営改革の手段となる可能性がある。

1. はじめに

2003年5月に公布された「個人情報保護法」にもとづき，2005年4月から，国の行政機関や独立行政法人等に続き，企業に対する「個人情報保護法」の適用がスタートし，「個人情報保護法」の全面施行が実現する。同法に違反した企業に対しては，「6月以下の懲役，または30万円以下の罰金」という法的罰則が課されることになる。

新たに「個人情報保護法」の義務規定の対象となるのは，5,000件を越える個人情報を検索可能な形で体系的に構成した「個人情報データベース等」を事業活動に利用している企業である。

☆(株) NTTデータ経営研究所

この「個人情報データベース等」には，コンピュータ処理情報のみならず，インデックスなどをつけた状態で管理された紙情報も含まれるが，問題は電子媒体にある。紙媒体のアナログ情報に比して電子媒体のデジタル情報は，更新，検索，名寄せ，複製などあらゆる点で，その利便性において，圧倒的に勝る。その利便性のゆえに，管理面での脆弱性もまた大きな問題となるのである。

「個人情報保護法」の施行は，企業にとっては経営コストの増加と経営自由度の低下というマイナスの文脈で語られることが多いが，ホンダやキャノンの環境規制の克服事例が示すように，このような規制が企業の技術・事業・経営革新を生み出し，競争優位を築く可能性があることを忘れるべきではないのではないか。

本稿では，最近の内部情報セキュリティ管理ツールの発展動向と企業の先端的導入事例の分析を通して，内部情報セキュリティ強化を企業パフォーマンスの向上につなげることが如何にしたら可能であるかの試論を試みたい。

2. 「外部からの侵入」と「内部情報漏えい」

これまでも個人情報の漏えいは，企業イメージの低下，売上減，損害賠償金の支払いなど，企業経営上の大きなリスクであったが，個人情報に関する社会的認知が上がり，「個人情報保護法」の適用により，さらに法的罰則が加わるといった企業を取り巻く環境の変化のなかで，企業ブランドの観点からの情報漏えいの抱えるリスクは企業にとって格段に高まってきているといえる。

これまでの情報セキュリティ強化の力点は，コンピュータと通信の融合によって，情報システムのネットワーク化が急速に進む中で，情報システムへの外部からの侵入にあったといえる。そして，外部からの物理的な侵入，および情報システムに対する不正アクセスに関しては，いくつかの有効な対策が考案され，実行されるようになってきている。しかし，現在企業が直面しているのは，個人情報漏えいの多くは「内部漏えい」が原因であるという点である。「内部漏えい」防止は，「外部からの侵入」を防止する場合に比べて，大きくふたつの難しい問題がある。実際，「内部漏えい」という社員の不正行為に対する企業の対策はかなり遅れているのが現状である。

ひとつは，システム的な難しさである。外部からの不正アクセスに対しては，アクセス制御等，情報への入り口をガードすることなどで防止可能であり，有効な対策を講じることができる。しかし，社員，即ち，使用を許可され正当な権限を有する者による意図的な情報漏えいの場合は，そもそもアクセスが不正であるかどうかの判断を行うことが非常に難しい。例えば，顧客名簿を印刷することを許可されている社員が，その印刷された個人情報を他の人間に売却すれば不正行為であるが，業務上の必要から内部会議などで使用するのであれば，通常の業務の範囲内であり，不正行為ではない。つまり，該当する行為，この例では印刷操作が行われた段階で，不正かどうかを判断することは極めて困難なのである。その一方で，情報を持ち出す方法も情報技術の急速な進歩によって容易化，多様化してきている。そのため，窮余の策として，通常の勤務時間帯以

外でのデータのダウンロードや印刷行為をチェックし，場合によっては，そのような操作を行おうとした時点で，使用中のパソコンの操作を不能とするツールを導入している企業もあるが，条件設定が難しく，業務効率の低下も考えると，必ずしも現実的な対処策とはいえないのが実情である。

もうひとつの問題は，業務効率と社員のモチベーションの低下である。「内部情報セキュリティ強化」のために，むやみに情報へのアクセスや情報機器の使用を制限してしまっては，情報へのアクセスの利便性を犠牲にして業務の自由度を下げてしまい，社員の業務に支障をきたすという本末転倒な結果となる。また，厳格な管理は社員の行為を制限・監視することになり，社員のモチベーションが大幅に低下する恐れがある。

3. 内部情報セキュリティ確保のためのITツールの現状

しかし，このような企業の「内部情報セキュリティ強化」というニーズを背景として，内部情報セキュリティ確保のためのITツールの積極的な開発が進んでいる。ここで，その現状を簡単に整理しておく。

ITツールには，機能別に大きく分けて以下の4つがある。

① **ネットワーク上のパケットログを監視・分析するための「ネットワークパケットチェック」ツール**：社内ネットワークを流れるパケットをログとして保存する。クライアントPC単位で，メールの送受信内容やサーバ上のファイルへのアクセス内容等がログとして残るため，ログ情報を監視・分析することで，それぞれのクライアントPCで行われたおおよその操作を把握することができる。

② **WindowsのAPIレベルでアクセス・操作ログを管理し，また操作制御を行う「Windows APIチェック」ツール**：ソフトウェア割り込みにより，アプリケーションの起動，ファイル名の変更や印刷，カットアンドペースト等の画面操作など，クライアントがPC上で行った操作をログとして保存する。「ネットワークパケットチェック」での記録情報（「どのPCから，何時，どのファイルにアクセスした」）に加えて，より詳細な情報まで記録されるため，不正操作に対して，より高い抑止力が働き，より正確な追跡調査が可能となる。

③ **やりとりする情報の内容を当事者以外に解読できないようにする「暗号化」ツール**：やりとりする情報の内容を当事者以外に解読できないよう，文字や記号を一定のルールで置き換え（暗号化），元に戻す（複合化）方式。暗号化されたファイルは一般的に検索が不可能であり該当ファイルを探しあてるのに手間がかかるため，不正操作の防止に効果がある。また，たとえファイルが外部に流出しても，複合化のルール（複合キー）が分からなければ情報を解読することができない。

④ **操作者がポリシーに違反した挙動や想定外の挙動を行った場合にキーボード操作を無効にする「キーボードのストロークチェック」ツール**：ポリシーに違反した操作や想定外の操作

等を行った場合，キーボードのストロークを無効にする。想定外のPC操作に対して強制的にキーボードロックをかけることにより，不正操作の防止を行うことができる。

これら4つのITツールはそれぞれに特徴があり，目的に応じた使い分けが必要であるが，内部情報管理のベースラインである情報漏えいの抑止という効果はある。しかし，もう一歩踏み込んで，誰がどのような操作を行い，どのデータを，どのような形で取り出したかを記録する方式であると，そのログを分析することにより，不正行為が行われた後に，誰が実行したかを簡単に特定することができる。それが，「Windows APIチェック」ツールである。「ネットワークパケットチェック」ツールでも，パケットログの取得は可能であるが，コピーやプリントアウトといったクライアントでのアクセス・操作ログを取得することができないのに対し，「Windows APIチェック」ツールでは，誰が，どのような操作をしたか，というログの取得が可能なため，非常に詳細な追跡が可能となる。このツールは，正確で詳細な「追跡力」という点でもっとも効果を発揮する。

ログ取得は，一義的には，情報漏えいへの対策であり，社員監視という表現に現れているように，マイナスの側面が強調されがちである。また，何もおきなければ，単に膨大なログデータを蓄積するだけであり，必要なこととはいえ，システムのパフォーマンスにもある程度の影響を与えるので，導入を躊躇する企業があっても不思議ではない。しかしながら，実際には，収集されたログは，これから説明するように他の分野への活用が可能であり，なおかつ，多少の犠牲かつコストを払いながら取得したものであるから，活用すべきものでもある。それどころか，ログを積極的に活用することにより日常の業務に多大な貢献をもたらすという，プラスの側面を引き出すことが可能となる。つまり，個人情報保護法を契機に，「情報」という企業にとっての未知の膨大な資産を活用するということが可能になるのではないか。実際，一部の先進的企業では，ログを積極的に活用することにより，業務刷新や組織再設計を行い企業パフォーマンスの向上につなげているところがある。

4. 内部情報セキュリティツール導入事例

ここで，「Windows APIチェック」ツールの導入の事例をいくつか紹介する。

事例1：機器メーカA社において，ある事業部が別会社として分社する際，退職する社員による顧客情報の持ち出しが発生し，顧客を横取りされるという事件が発生した。雇用状況の変化から，社員退職時の情報持ち出しは今後増加する可能性が非常に高いが，通常のパケットログのみでは，アクセスしたことを証明することは可能であっても，コピーによる持ち出しやプリントアウトによる持ち出しを証明することは不可能である。したがって，このような事件が発生した場合，企業は損害を受けながらも手を打てないことが多い。しかし，この企業では「Windows APIチェック」ツールによるアクセス・操作ログを取得していたことにより，その退職者

が顧客データベースにアクセスし，外部に持ち出すまでの一連の行為を正確かつ詳細に追跡し，迅速な事後対処を行うことができたのである。A社では，客観的な事実としての「内部操作ログ」は，万が一訴訟に至った場合の証跡としても非常に効力を発揮するであろうとしている。

事例2：金融資産管理企業B社は，プロフェッショナル組織であり，内部情報セキュリティ強化を実施する際の大前提として，「業務の自由度と情報アクセスの利便性を落とさないこと」を定めた。この大前提のうえでB社が考えた第一のポイントは，「インターネット時代にふさわしい情報セキュリティ対策を講じる」という点であった。そして，第二のポイントは，「性善説にたった情報セキュリティ対策を講じる」という点であった。性悪説にたって情報管理を行おうとすると，どうしても“情報にアクセスさせない”，“情報を見せない”という硬直的な管理をせざるを得なくなる。これでは，業務効率が大幅ダウンすることは明らかである。

こうした観点からB社では，「情報漏えい対策の根幹は『発信者責任』にある」との結論に達した。そこで，B社が導入したのが「Xドライブ」（仮名）という暗号化除外フォルダである。「Xドライブ」とは，社員が“うっかり（つまりXドライブを経由せずに）”ファイルを外部へ流出させてしまった場合には，情報の受け手は情報を見ることができないという仕組みである。この仕組みを用いることで，硬直的に情報を暗号化する場合とは異なり，「業務自由度の維持」と「内部情報のセキュリティ強化」を両方することができた。

とはいえ，詳細なPC操作まで監視される「Windows APIチェック」ツールの導入は社員にとって気持ちの良いものであるはずはなく，下手をすると社員のモチベーションを大きく低下させるリスクをはらんでいた。ここでB社がとった方策は，担当者を一方的に監視するではなく，経営トップや管理職に対しても“監視”を行うというものであった。この方針は，経営層が情報セキュリティに対して“本気”で取り組むという決意の表れであり，社員にもこの決意は自然と浸透していったという。

B社の対策のもうひとつの特徴として，「Windows APIチェック」ツールにより取得される「アクセス・操作ログ」を，情報システム部門ではなく，各現場の部門長が管理・参照しているという点がある。この理由は，情報の機密性は固定的なものではないため，情報システム部では情報の機密度・重要度に対する判断は不可能である，との認識からであった。

こうした取り組みにより，B社ではプロフェッショナル組織にふさわしい情報セキュリティ対策を講じることに成功したのである。なによりの効果は，「Xドライブ」を導入したことにより，社員の情報セキュリティに対するリテラシーが飛躍的に向上したことであった。情報を外部に発信するたびに，ファイルをXドライブ経由で送信するという“ひと手間”が存在することは，一見，社員の利便性を損なうように思われる。しかし，この“ひと手間”こそが，社員が常に「情報セキュリティ」を意識するきっかけとなり，その結果，情報漏えいが防止されただけでなく，社員のひとりひとりが情報セキュリティについて意識するようになり，社員の情報リテラシーが飛躍的に向上したのである。

事例3：電子部品メーカC社では，「Windows APIチェック」ツールを導入したことで，当

初80名ほどであった部署を，最終的には十数名規模にまで人員削減することに成功している。約5倍近い生産性向上である。社員が減ると，当然，事務スペース，備品，福利厚生費等の経費も削減できるわけであり，コスト削減という点から見ても，このインパクトがいかに大きいかは容易に理解できる。

これはいかにして可能となるのか。まず，「Windows APIチェック」ツールは個人のPC操作の一挙一動を明らかにするため，ネットサーフィンやネットゲームなど，業務以外のことに費やすことはよほどでない限り不可能となり，勤務時間は100%業務に集中するという環境ができあがる。この時点で不正な操作が淘汰されていることはいうまでも無い。次に，「アクセス・操作ログ」の分析により無駄な業務プロセスや処理を見つけ改善することで，業務の生産性があがる。そして最終的には，おそらくこれがもっとも肝心なことであるが，職場に徹底した「生産性」の原理を導入することで，そもそも不正を企てる社員や怠惰な社員が自然淘汰され，さらに生産性がアップする，という仕組みである。

つまりこの企業では，「Windows APIチェック」ツールの導入により，内部セキュリティの強化はもちろん，「Pay for Performance」，厳然たる指標で社員のパフォーマンスを測り，これにより給与を支払うという経営改革を実現したのである。「セキュリティとは，つまるところ，人間教育。人間教育を徹底すれば，セキュリティ対策は本来不要となり，最終的には，究極の生産性向上が実現できる」とは，このC社の社長の言葉であるが，内部情報セキュリティの強化がもたらす正のインパクトを見事に言い表しているといえる。

もちろんこうした経営改革は，社員に対する締め付けだけで実現できるわけではなく，この企業では，社員に対してかなりの給与格差を付ける一方で雇用も確保している。また食堂や職場環境などでも社員への気配りを忘れていない。

事例4：運輸機器製造メーカD社にとって図面やマニュアルは自社のノウハウそのものであり，こうした情報が外部へ流出することは致命的な損害となる。こうした観点から，従来D社では，図面やマニュアル類の情報を全て非公開としていた。しかし，「Windows APIチェック」ツールによりアクセス制御や操作ログ取得が可能となり，コピーやプリントアウトによる持ち出しから情報を守ることができるようになったため，これまで共有を許可していなかった図面やマニュアルを，関連他部署と共有することを決めた。

この結果，当初は図面やマニュアルを閲覧することのできなかった部署に所属するエンジニアが，重要かつ先端の技術を含む図面やマニュアルを閲覧することが可能となり，また部署をまたがるメンバ間で図面をみながら議論することも可能となった。このようにD社では，的確な情報セキュリティ対策を講じたからこそ，本来共有すべきメンバー間で情報を共有し，知的協業を展開することにより新たなアイディアがうまれ，価値を生むことに成功している。

事例5：アパレルメーカE社では，「Windows APIチェック」ツールを導入したことにより，ウェッブページの閲覧時間が約半分に減少したのみならず，延べアクセス人数上位20%にあるファイルに全アクセスの80%が集中していることを突き止めた。この結果から，どれほど不正

なウェッブページの閲覧がなされているか，また社内にどれほどの不要なファイルが保存されていたかということを把握することができた。今後は，閲覧頻度の高いファイル精度を操作性も含めて高め，閲覧されていないファイルは削除することにより，情報資産の効率的な運用を目指している。この背後には，不要な情報資産で削減したコストを有益な情報資産に再投資するという考え方がある。

また，アクセス・操作ログ分析の応用として，これまでは社員の要望によりシステムの開発が行われてきたが，アクセス・操作ログを分析することにより利用状況を把握することができるようになった。つまり，アクセス・操作ログが社員の要望に対して「本当に必要なのか」「どの程度重要なのか」といったことを，定量的に検証することを可能にしたのだ。

さらに，E社では，「Windows APIチェック」ツールによるアクセス・操作ログをもとに，パフォーマンスの高い営業担当社員がどのような情報をどのように利用しているのか，といった操作手順を可視化し，さまざまな角度から分析しテンプレートとして再現性をもたせることで，企業パフォーマンスのベースラインを高めることが可能ではないかと考え，テンプレート化の検討を継続的に行っている。アクセス・操作ログの取得により，いかに情報の提供や共有を呼びかけても収集することの難しかった情報を収集することが可能になったことは，非常に大きな意味を持つといえる。

事例6：電子部品メーカF社では，「Windows APIチェック」ツールの導入により，チームメンバーの作業進捗を効率的に把握し，作業ロスや納期の遅れを未然に防ぐことに成功している。

一般的に，チームリーダーにとって，チームの進捗管理は，実は，各サブチームリーダーからの報告に頼る部分が大きく，また進捗遅れの理由を正確に把握することは困難である場合が多い。しかしながらF社では，「Windows APIチェック」ツールを導入しチームリーダーが「アクセス・操作ログ」を見ることで，個人の作業進捗状況をリアルタイムに把握し，滞っているタスクを容易に洗い出すことが可能となった。この結果，メンバー間の進捗齟齬による作業ロスを最小限に抑え，また納期直前に想定外の進捗遅延が露見するといったリスクを未然に防ぐことに成功している。

5. ログ活用の類型化

上記の事例から，情報セキュリティツールを通して蓄積されるログの活用およびその効果を類型化してみることにする。

ログ活用の第一は，余剰IT関連資産と余剰人員の発見である。データアクセスや操作ログを分析することにより，ほとんどアクセスされない無駄なデータが大量にあることがわかり，その分のストレージやCPU，さらに運用の人件費を削減できる。実際，よく言われるように頻繁にアクセスされるデータは，全体のごく一部であることが判明する。もちろん，アクセス数が少ないからと言って，必要なデータまで削除することはできないが，ワーキング（下書き）資料や作

業用データ，古いバージョンのセールスツールなど，すでに保管しておく必要がないデータが，大量にストレージ上に存在しているケースが多い。

また，アクセス・操作ログの分析から，個人の作業の無駄や進捗の管理にとどまらず，業務の実操作時間を計測し，それに基づいて，想定標準作業時間および必要要員数を算出し，余剰人員の削減が可能となる。もちろん，すべての作業をシステム上で実施しているわけではないが，業務遂行上，必要となる作業時間・人員数を概ね算出することは可能であり，より適正に近い人員配置を設定することが可能となる。

ログ活用の第二は，操作性の改善である。ログ情報を分析すれば，個々の操作者が，どのような手順で，画面を操作しているのかを把握することが可能となる。それにより，設計段階において，想定していた操作手順とは異なった操作が多いなどということが相当数発見される。このような場合，手順に変更を加えたり，バイパスを設定することにより，操作性を改善することが可能となる。なかには，操作方法の教育や操作マニュアルが不十分なために，もっと適切な操作があることを知らない場合もある。経理や人事等の社内業務であれば，手順の多さによる作業時間の増加は，会社の業績に大きな影響を与えないが，例えば，コールセンターの場合，多数のオペレータが数種類の操作に従事しており，複数の同一作業が相当数繰り返されていること，顧客への返答（レスポンス）時間が顧客満足度に影響することなどから，このGUIの操作性の改善は，オペレーション効率上，極めて需要な課題と言える。

ここで重要なことは，GUI設計の基本でもあることだが，ほとんどすべての操作を効率的に行えるようにする必要はない。頻度が高い作業およびクレーム対応など緊急性を要する業務に関連する操作を効率的に行えるようにすればよい。このような場合に，取得したアクセス・操作ログの分析を活用すれば，業務の実態を把握し，改善策を実施することが可能となる。取得ログから現実に行われている各業務の業務量・頻度，重要性等を分析することにより，効率的な業務を実現できるように，GUIを改善し操作を効率化することにより，顧客対応のスピードアップが図られ，顧客満足度が向上することが期待できる。

ログ活用の第三は，業務パフォーマンスの向上である。この領域は営業現場がもっとも有効であろう。営業は最もITから遠い領域といわれているが，近年，情報システムが積極的に導入されるようになってきている。営業現場での支援系のツールの利用に関するログと，営業行動のシステムへの登録情報を分析することにより，その営業担当者の営業行為・パターンが推測可能となる。営業担当者を，成績で上・中・下と分けると，上位のグループの営業パターンは，下位のグループとは異なっているはずである。上位のグループのツールの利用プロセスは，無駄がなく，論理的なつながりがある。それに対して，下位のグループの利用プロセスには，無駄が多く，繰り返しや後戻り，誤った営業ツールの選択などが発見されるはずである。また，営業行動にも，無駄や意味のないものが散見されるであろう。グループ単位で，それぞれの特性を分析し，上位のグループと下位のグループを比較することにより，下位グループの問題点をより明確にすることが可能となる。また，上位グループの分析結果から，下位グループがどの部分を改善すればよ

いかが明らかになるはずである。パフォーマンスの高いグループのナレッジを可視化して，テンプレート化することで，トランスファーすることも可能となる。

以上で類型化を試みた取得可能なログの活用は，現在販売されているセキュリティツールのどれかひとつの製品で全て実現できるわけではない。現時点では，複数製品を組み合わせて使用するか，そのようなセキュリティソリューションサービスを受けることになる。特に，ネットワークログやパソコン上のアクセス・操作ログなどは取得可能だが，データベースへのアクセス・操作ログの取得に関しては，それほど良いツールは存在しないのが現状である。ERP パッケージ等も含むアプリケーションレベルにおいては，上記の目的に合ったログ取得は，ほとんどされていない。

セキュリティ・ツールには，ノートパソコンを暗号化などでロックして，所有者以外が操作不能とすることにより，盗難に備えるとか，EXCEL などのファイルを印刷不可にするなどの対策を前提にしたものが多いようであるが，大量に個人情報を保持している企業の場合，そのデータはデータベースに格納され，アプリケーションを用いてアクセスする使い方が一般的である。従って，正当な権限を有する社員が個人情報を入手するルートも，アプリケーションを通じてのデータベースアクセスを通してである。また，前述した営業現場においても，アプリケーションを使用する機会は増えつつある。

6. 内部情報セキュリティツール導入によるパラダイムシフトのステップ

以上の事例やアクセス・操作ログ活用の類型化を通して，内部情報セキュリティの強化が企業に与える影響を「マイナス」から「プラス」に転換することが，セキュリティツールの導入とその使い方次第で可能であることが明らかになった。本稿のまとめとして，パラダイムシフトにつながる経営革新へのステップを試論的に定義してみることとする。

ステップ1：情報セキュリティリテラシーの向上

第一のステップは，内部情報セキュリティリテラシーの強化である。事例1に示したように，「Windows API チェック」ツールを導入していた企業では，退職した社員による顧客情報の持ち出しが発生し，顧客を横取りされるという事件が発生した際，アクセス・操作ログの分析から，一連の不正行為を特定できた。これは確かに利点ではあるが，やり方を間違えると，厳格な社員監視という負の影響，つまり社員のモチベーションの低下をもたらす危険性が多分にある。それを避けるために，事例2と事例5が示すように，まず，情報セキュリティ強化の必要性とそのルール化を全社できちんと共有することが重用である。欧米のようにビジネス・コンダクト・ガイドライン（BCG：企業内部行動規範）が明確ではない日本企業では，個人情報保護法の導入を契機とした内部情報セキュリティ強化を利用して，企業内部での行動倫理についての議論を行うのは，企業のインターナルコントロールの観点から非常に有意義である。また，このような内部情

報セキュリティツールの導入は，情報システム部門に任せるのではなく，トップ・マネジメントの強いコミットメントのもとで行うことが必須である。

このステップで特に重要なのは，情報セキュリティに関する社員のリテラシーの向上である。このリテラシーの向上は，情報セキュリティへの急速な関心の高まりから，ISMS認証取得や内部情報セキュリティソフトの導入など適切な情報セキュリティ対策が行われていることを取引の要件とする企業が増えてきているという事実からも伺われるように，ビジネスの観点からも強く求められている。

ステップ2：オペレーションの最適コントロールとコスト管理

このステップは，アクセス・操作ログの取得とその分析によって，日々のオペレーションの無駄を排除し，徹底的な効率化とその適正化を目指すものであろう。これは，コストの削減に関わるものであり，情報技術を活用していることからも分かるように，対象は，従業員が関わる業務ばかりでなく，情報システムにかかわるIT資産も含まれる。

事例3，5，6が示すように，「Windows APIチェック」ツールによるアクセス・操作ログを分析すれば，上司からの指示やタスクの進捗状況から，インターネットの私的利用や業務効率の低さまで各社員の生産性状況がかなり明確に把握することができるようになる。このことから，残業などのコスト削減や職務怠慢の防止という非常に初歩的な無駄の排除を期待できる。また，アクセス・操作ログの取得によって，各情報に対する利用頻度が明らかになるため，不要なファイルを削除することでハードウェアやデータベースなどの余剰IT資産コストの最適化をはかることもできる。

さらに，アクセス・操作ログで社員の勤怠状況を分析することによる現行業務内における無理や無駄を把握できる。また，その分析から，実操作時間を計測し，想定作業時間および必要要員数を算出して，適正に近い人員配置をおおよそ推定することができる。これらを比較することで，余剰人員の削減を実施し，業務プロセスの適正化をはかることが容易となる。つまり，余剰人員削減と業務プロセスの最適化と人員の適正配置が可能となるのである。

製造業的感覚でいえば，製造現場でのブルーカラーの管理をホワイトカラーにも適用することを意味している。ホワイトカラーといっても，創造的な仕事をしているホワイトカラーは商品開発，研究開発部門，一部の営業，専門職といったむしろ限定的なものであり，間接部門のかなりの人員は，擬似定型作業が多いので，ブルーカラー的な管理に馴染まないとはいえない。「Windows APIチェック」ツールのような情報セキュリティツールの出現によって，「本来すべきであったができなかった」ことが可能になったというのが，製造業の経営者の認識である。ただし，ホワイトカラーの人々からすれば，「**ホワイトカラーのブルーカラー化**」に拒否反応が強いことも事実であるので，ホワイトカラーの業務の大半がブルーカラーに近い擬似定型作業であったとしても，モチベーションの観点からの考慮は必要であろう。

ステップ3：企業の保持する情報の資産化

第3のステップは，より積極的は段階である。ステップ2が，オペレーションの効率化であるとすると，ステップ3以降は，効果性の問題である。つまり，ITツールの導入を契機に，社内ドキュメントの「情報資産」化を進めるステップである。

ITツールを導入するには，当然のことながら，まず，多くの場合社内データベースに散乱・放置されている個々のドキュメントについての有益性を評価し，不要なドキュメントの削除（これは，ステップ2の効率性の議論である）および有益なドキュメントに対するアクセス・操作権限を設定する必要があるが，そこからさらに進んで，有益なドキュメントを業務アクションや商品毎に連携させることで，ドキュメントを「情報資産」として整備することが可能である。また「情報資産」の利用実績をアクセス・操作ログにより分析することで，資産として常に最適な状態に維持し続けることも可能である。事例5が示すように，GUIの操作性改善もこの例であろう。アクセス・操作ログ情報を分析すれば，操作者が，どのような手順で，画面を操作しているのかを把握することが可能となる。それにより，無駄な操作や誤った操作など，設計段階において想定していた操作手順とは異なった操作が多いなどということがわかり，手順変更を行うなり，バイパスを設定することにより，操作性を改善することが可能となる。このようにして，最適なGUIを維持・更新し，GUIという情報資産の価値を高めていくことが可能である。つまり，情報利用者による「より良き情報は，より良く，不要なものは淘汰される」という「情報の価値は他者が判断する」という原則の運用を確立できる可能性が出てきたのである。事例5が示すように，削減した余剰IT関連資産のコストを有益な情報資産に再投資し，動的な好循環サイクルを構築するという選択的なIT投資が可能となる。ステップ2で行う余剰IT関連資産の削除という静的な対応では，情報資産の価値を維持・向上させていくことは難しいが，このステップ3によって，情報資産の価値を維持・向上させていくことが可能となる。

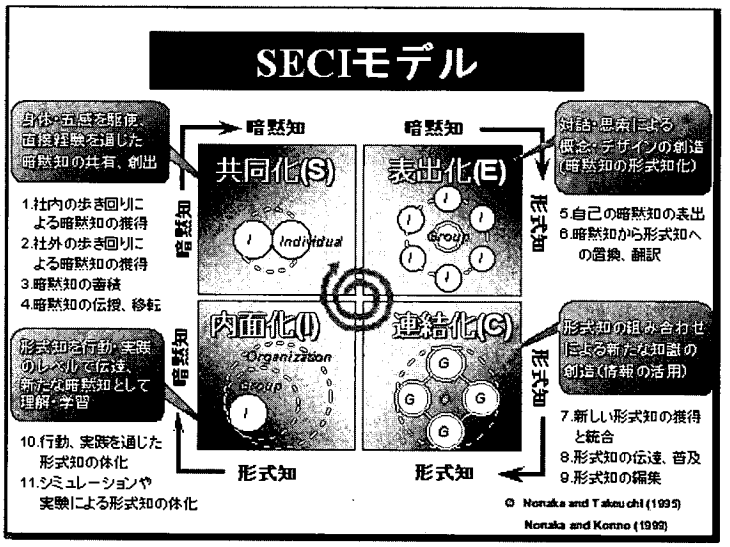
これまでにも企業の保持する情報の価値とその活用についての議論はなされてきているが，私見では，「べき論」か「希望論」であり，実現化されたケースを耳にしたことはない。企業の保持する情報は，企業にとって企業資産としての最後の未知なる大陸であるのは事実である。昨今の内部情報セキュリティの強化と情報セキュリティツールの進歩は，企業における最後の未知なる価値を，資産化しうる可能性をはるかに高めたといえる。今後，社内保有情報の資産化の成功の有無が，日本企業の成否を分ける可能性が高いのではないか。また，こうした情報資産やIT資産の上手な活用実績は，企業のブランドイメージも向上させ得る。この段階まで進めば，社員の日常業務に対して目に見えるメリットがもたらされるため，内部情報セキュリティの強化によるモチベーションや生産性の低下を心配する必要はないであろう。

この意味で，ステップ3は情報というものに対する企業のattitude（姿勢）を根本的にかえるパラダイムの転換のステップと理解することができる。この姿勢の転換は，ステップ3以降の情報をベースとした価値拡大を実現化していくうえで必須といえる。

ステップ4：オペレーションレベルにおけるナレッジトランスファーとナレッジシェアリングの可能性

野中も指摘しているように，SECIモデル(1)（**表1**）において，個人や組織が体で覚え，共有・統合された知識を言語のような明示的な形式で表わす**Externalization**（表出化）のフェーズは，暗黙知から形式知への転換であり，最も難しい転換フェーズである。確かに，新製品開発やR＆D関連では，プロトコルの共有やコミットメントもあり組織等質性や共通目的も明確であり，比較的ナレッジトランスファーとナレッジシェアリングが可能な環境にあるといえる。事実，事例4が示すように，情報セキュリティ対策を施すことで，開発部門が，これまで共有することが

表1



（1） SECIモデルとは，「組織において知識が創造されるには次の4つの知識変換プロセスがある」とする野中郁次郎教授（一橋大学院国際企業戦略科）のモデル概念である。SECIとは，Socialization（共同化），Externalization（表出化），Combination（連結化），Internalization（内面化）の4つのプロセスの頭文字からとられたものである。このモデルでは，この4つのプロセスが，相互に作用して一段上の知識レベルへ昇華するプロセスを理論化したもので，1991年にハーバード・ビジネス・レビューにて初出されたものである。

- Socialization（共同化）とは，親から子へ，先輩から後輩へ，あるいは熟練者から未熟練者へと共通の経験を共有することにより，言葉によらずに体験によって，知識を伝授し獲得するプロセスを言う。所謂，「身体で覚える」というものである。
- Externalization（表出化）とは，このように個人や組織が体で覚え共有・統合された知識（暗黙知）を言語のような明示的な形式で表わすことを指す。
- Combination（連結化）とは，Externalization（表出化）によって明確になった知識（形式知）を組合せて新たな知識を創るプロセスである。
- Internalization（内面化）とは，このようにして得られた知識をもとに個人が行動し，実践することによって，新たな経験や学習結果が個人の内部に蓄積される状態を言う。この段階では文章などに表わして他人に伝えることができない体験や主観といった非明示的な知識として蓄積される。

SECIモデルにおいては，S→E→C→I→S→E→……と知識の蓄積プロセスが循環することにより，組織およびその構成員である個人の知識レベルがより高いレベルに到達・昇華するとされ，これを「知識創造スパイラル」と呼んでいる。

できなかった図面やマニュアルを共有したことにより，ビジネス上の新たなアイディアの創出に成功しており，ITを駆使した情報セキュリティ対策の強化が開発という限定的な領域であるが，ナレッジマネジメントへ寄与しうる可能性を示唆している。

しかし，日々のオペレーション・ベースのナレッジの **Externalization**（表出化），つまり，ナレッジトランスファーは非常に難しいのが現実といえる。しかし，「Windows API チェック」ツールにより記録される「アクセス・操作ログ」の分析が生み出す価値を活用することにより，このオペレーションレベルでのナレッジトランスファーの可能性が出てきたと考えられる。

「アクセス・操作ログ」には，クライアントPC操作者の起動アプリケーション，ファイル操作，Webアクセスなどの操作履歴が詳細な形で残されるので，この履歴情報は，実は，個々人の業務プロセス（暗黙知）をもっとも“正確”かつ“自動的”に反映したものである。従って，優秀といわれる（特に営業関係の）社員の「アクセス・操作ログ」と彼/彼女のパフォーマンスの相関関係を検証し，「操作」パターンを解析し，そこに潜む暗黙知を表出化し，組織としての業務プロセスのベストプラクティスとして，テンプレートのような形で共有化することが可能となる(2)。従来のナレッジマネジメントは，ナレッジの「自主的な提供」あるいは「偶然的」ナレッジを前提としていた結果，Know Who か知識の形骸的なトランスファーにとどまっていたが，これを，「アクセス・操作ログ」をベースとすることで，アップワードスパイラルな形での価値あるナレッジトランスファーとナレッジシェアリングの仕組みへと転換させる可能性がでてきたということである。事例5が示すように，最終的には暗黙知のテンプレート化（形式知化）を目指す企業が現れ始めており，これまで非常に困難であったオペレーションレベルでの暗黙知の形式知化（**Externalization**：表出化）が可能になろうとしている。このテンプレートをオペレーショのベースとして継続的に使い，「アクセス・操作ログ」をさまざまな角度から分析してテンプレートの精度と価値を高めていくという考え方は，企業のパフォーマンスを高める上で非常に有効な手段であるといえるのではないか。

ステップ5：業務・人材・組織刷新による HPO(High Performance Organization)の設計

ここまでアクセス・操作ログの分析による企業経営に対するインパクトをステップ化して検討を試みたが，ステップ4までは，既存の組織経営の枠組みの中での議論であった。しかし，ステップ4までの進展を突き詰めて考えると，内部情報セキュリティの強化と「アクセス・操作ログ」の分析で，職場に徹底した「生産性」の原理を導入することで，そもそも不正を企てる社員や怠惰な社員が淘汰され，さらに生産性がアップするという選別の仕組みに行き着きはしないであろ

（2）確かに，膨大なアクセス・操作ログやネットワークログを解析することにより，どのような操作が行われたかを類推することは可能だが，アプリケーションレベルでログを取得すれば，その点に関しては，よりシンプルかつ直接的なログ情報を取得できるわけであり，アプリケーションレベルでのログ取得はかなり重要といえる。今後，情報漏えい対策のためにも，さらに，ログを積極的に活用するうえでも，データベースへのアクセスログの取得やアプリケーションレベルでのログの取得が実現されることが期待される。

うか。つまり，アクセス・操作ログの分析を利用して，厳然たる指標で社員のパフォーマンスを測り，これにより会社に対する寄与度に応じて給与を支払うという企業のメリット・ベースによる「Pay for Performance」が実現できるのである。「セキュリティとは，つまるところ，人間教育。人間教育を徹底すれば，セキュリティ対策は本来不要となり，最終的には，究極の生産性向上が実現できる」とは，事例3で取り上げた企業の社長の言葉であるが，これは，言い換えれば，情報セキュリティを含むビジネス・リテラシーもパフォーマンスも高い社員をベースとして，既存組織を見直し，「Pay for Performance」を前提に業務・人材・組織を刷新して，組織効率の極めて高いHPO（High Performance Organization）を実現するという経営改革を意味してはいないか。

この流れは，日本企業組織のアングロサクソン化を促す新たなモメンタムと捉えることもできる。しかし，その前に議論をしなければならない問題が二つある。ひとつは，「Pay for Performance」に関してである。「Pay for Performance」は，確かに上記で論じた選別を通してやりやすくなるのは事実であろう。しかし，そもそも「Pay for Performance」の背景には，企業にとっての「メリットベース」というアングロサクソン的組織設計思想があり，従業員の「ニーズベース」を暗黙の組織設計思想としてきた一般的日本企業において，「成果主義による二極化の進行」（城，2004年）が何らかのセーフティネットを抜きにして，このまま続くのかは，議論の分かれるところではないだろうか。

もうひとつの問題は，組織帰属性と組織力の問題である。この「Pay for Performance」の流れは，「従業員と企業との関係は，従業員の提供サービスにたいする金銭対価の最大化であり，それ以外の組織帰属性やコミットメントは重要な問題ではない」という認識を助長する。現在のアングロサクソン社会における金融業業界がその典型であろう。アングロサクソン系の企業は，究極のビジネスマシンを造ることを目標としている。マイクロソフトは，ログの解析とカメラを使用して，ホワイトカラー版のテイラー分析サービスを開始し，一層の効率的ビジネスマシン構築を支援し，サン・マイクロシステムズ日本法人は，社長室も含めて社員9割の固定席の廃止によるオフィスの効率化で5億円を節約し，ビジネスマシンとしての効率を高め，企業と従業員とのつながりは，「Pay for Performance」に収斂させていくように思える。他方，アングロサクソン社会における個人は，自分の能力に依拠して「組織に雇われない生き方」（Pink, 2001）や「個人の自由，創造性，価値観を中核に据えた組織」（Malone, 2004）の方向に向かっている。

しかし，日本人の組織帰属性は，欧米とは大きく異なる。カール・ポラーニの言うところの「埋め込み」は，生まれながらの半ば所与の関係である西欧的な帰属的社会的関係をさしているのに対して，日本での「埋め込み」の対象となる帰属的社会的関係は，後天的に獲得される企業という経済活動が行われる場でさえも含む。これが，日本社会における個人と企業組織の関係をユニークなものとしている。戦後の日本企業の組織力を担保してきた，この組織帰属性と日本人にとっての集団（組織）における役割の重要性（小笠原，2003年）を考えると，欧米型の「Pay for Performance」ベースによる効率的なビジネスマシンであるHPO（High Performance Or-

ganization）とは異なる組織帰属性と役割を明確化した日本型の「Pay for Performance」ベースによるHPO（High Performance Organization）のコンセプトの構築が重要なのではないだろうか。

7. 終わりに

負の影響が語られることの多い「個人情報保護法」と内部情報セキュリティの強化であるが，本稿で検証してきたように，内部情報セキュリティ対策は，昨今の環境経営などと同様に，企業経営のパラダイム変換を促す起爆剤ともなり得るのである。さらに，個人情報保護法の対象は，「情報」という無限の可能性を秘めたものである。「内部情報管理とは，社員の情報へのアクセスを制限することではなく，安心して情報を活用できる仕組みをつくること」であり，個人情報保護法を契機に，ITツールをうまく導入し活用することで，「情報」という企業にとって未知の資産を活用することができれば，企業競争力を大幅に向上することができるのではないだろうか。このことは，従来，IT（情報技術）に偏向していたCIOが，I（情報）に軸足をおく本来のCIOの機能を果たす必要性が高まることを意味している。つまり，企業において戦略的情報マネジメントの重要度がいっそう高まるのである。

最後になるが，企業や業界の特性によっては，本稿で論じた5つの発展ステップがすべて妥当ではない。また，この5つのステップは，試論の段階であり，今後の情報セキュリティツールの技術的発展と導入の事例の増加によって，更なる検証が必要である。

参考文献

小笠原　泰『日本的改革の探究：グローバル化への処方箋』日本経済新聞社，2003年

城　繁幸「『平等』『安定』を捨てた日本企業の迷走」『中央公論』2004年12月号　中央公論新社

Ikujiro Nonaka, "The Knowledge-Creating Company", Harvard Business Review, November, 1991

Ikujiro Nonaka, Hirotaka Takeuchi, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation,* Oxford University Press, 1995

Malone, Thomas W., *The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life,* Boston: MA, Harvard Business School Press, 2004

Pink, Daniel H., *Free Agent Nation: The Future of Working for Yourself,* New York: NY, Warner Books Inc., 2001

Polanyi, Karl, *The Great Transformation,* New York: NY, Rhinehart, 1944（『大転換』吉沢英成他訳，東洋経済新報社，1975年）